What is claimed is:

1. A mobile communication terminal that receives information received from a contactless communication tag, the mobile communication terminal comprising:

a first communication unit, which wirelessly exchanges data with the contactless communication tag and wirelessly sends a power required for the contactless communication tag;

a second communication unit, which transmits data to and receives data from a service management server via a wireless communication network;

a storing unit in which at least one encryption key related information are stored;

a decryption unit, which decrypts data received from the contactless communication tag based on encryption key related information that is selected from the encryption key related information by encryption key specifying information received from the contactless communication tag;

an information reading unit, which requests product information to the contactless communication tag attached to a product and reads the product information received from the contactless communication tag; and

an output unit, which outputs the read product information.

2. The mobile communication terminal of claim 1, wherein the encryption key related information includes at least one encryption key and the decryption unit decrypts product information received from the contactless communication tag by an encryption key selected based on the encryption key specifying information received from the contactless communication tag.

3. The mobile communication terminal of claim 2, further comprising a leaked encryption key updating unit that upon receipt of encryption key update request information concerning a leaked encryption key from the contactless communication tag, discards an encryption key designated by the encryption key update request information from the storing unit and updates with a newly assigned encryption key.

4. The mobile communication terminal of claim 1, wherein the encryption key related information includes a plurality of encryption keys that is classified and

assigned according to a classification reference including at least one of a type of industry, a manufacturer, a brand, and a product name; and

the decryption unit decrypts the product information received from the contactless communication tag using an encryption key selected from the plurality of encryption keys based on the encryption key specifying information received from the contactless communication tag.

5. The mobile communication terminal of claim 1, wherein the encryption key related information includes at least one seed value for creation of different encryption keys; and

the decryption unit decrypts the product information received from the contactless communication tag using an encryption key using a seed value selected based on the encryption key specifying information received from the contactless communication tag.

6. The mobile communication terminal of claim 5, further comprising a leaked seed value updating unit that, upon receipt of seed value update request information concerning a leaked seed value from the contactless communication tag, removes a seed value designated by the seed value update request information from the storing unit and updates with a newly assigned seed value.

7. The mobile communication terminal of claim 1, wherein the encryption key related information includes a plurality of seed values that is classified and assigned according to a classification reference including at least one of a type of industry, a manufacturer, a brand, and a product name; and

the decryption unit decrypts the product information received from the contactless communication tag using an encryption key created based on a seed value selected from the plurality of seed values based on the encryption key specifying information received from the contactless communication tag.

8. The mobile communication terminal of claim 1, further comprising a leaked encryption key updating unit that, upon receipt of update request information concerning leaked encryption key related information from the contactless communication tag, removes encryption key related information designated by the

update request information from the storing unit and updates with newly assigned encryption related information.

9. The mobile communication terminal of claim 1, further comprising a replay attack blocking unit which generates a one-time use random number, adds the one-time use random number to information to be transmitted to the tag reader, provides the information to the decryption unit, and checks if a random number extracted from information received from the tag reader is the same as the one-time use random number, thereby blocking replay attack.

10. The mobile communication terminal of claim 1, wherein the storing unit includes non-volatile memory, and further comprising a refresh processing unit that reads the product information from the storing unit and re-records the read product information on the storing unit.

11. The mobile communication terminal of claim 1, wherein a radio frequency (RF) circuit, the information reading unit, the decryption unit, and the storing unit of the wireless communication unit are implemented as application specific integrated circuit (ASIC).

12. The mobile communication terminal of claim 1, wherein the information reading unit specifies a plurality of product information from a type of industry, a manufacturer, a brand, and a product name based on the encryption key specifying information received from the contactless communication tag and provides the specified plurality of product information to the output unit, and the output unit outputs the specified plurality of product information.

13. The mobile communication terminal of claim 1, further comprising a reader authentication unit that authenticates an external mobile communication terminal having a tag read function by communicating with the external mobile communication terminal having the tag read function and outputs a result of authentication concerning the external mobile communication terminal having the tag read function to the output unit.

14. The mobile communication terminal of claim 1, further comprising an encryption unit that encrypts data to be transmitted to the contactless communication tag based on encryption key related information selected from the encryption key related information by encryption key specifying information received from the contactless communication tag.

15. The mobile communication terminal of claim 1, wherein the information transmitting unit adds purchasing information of a product to a result of determination if a purchasing confirm command is input through an information input means included in the mobile communication terminal and transmits the result of determination to the service management sesrver.

16. The mobile communication terminal of claim 1, wherein a result of determination is stored in the storing unit every time the product information is read; and

the information transmitting unit transmits the result of determination stored in the storing unit to the service management server if an information transmission command is input through an information input means included in the mobile communication means.

17. A method of managing product authentication service in a product authentication service management server that communicates with a subscriber server of a mobile communication company via a network and can communicate with a mobile communication terminal via a mobile communication network, the method comprising:

receiving reading detail information including a product identification number assigned to each product whose tag is to be read and a reader identification number assigned to the mobile communication terminal from the mobile communication terminal;

asking the subscriber server inquiry of subscriber information based on an identification number of the mobile communication terminal included in the reading detail information and receiving the subscriber information from the subscriber server;

creating and storing customer management information including subscriber classification information and product information reading details based on the reading

detail information and the subscriber information; and

reading and outputting the customer management information in response to an information output request that is input from an external device.

18. The method of claim 17, wherein the subscriber classification information includes at least one of age, area, sex distinction, and job of a subscriber; and

the reading detail information includes at least one of a type of industry, a manufacturer, a brand, a grade, a model name, a producing center, date and time of manufacture, a product serial number, a product price, and a time of authentication.

19. The method of claim 18, wherein the reading detail information further includes purchasing information concerning a product that has been already purchased, including a purchasing price and date and time of purchasing.

20. The method of claim 17, further comprising adding points of the subscriber according to the reading detail information.

21. The method of claim 17, further comprising checking repetitive transmission of information by checking if the product identification number and the reader identification number that are included in the reading detail information are the same as those included in reading detail information that is previously received from the mobile communication terminal.